## IN THE CLAIMS

Claims5, 17 and 29 are amended.

į			
	1	1.	(Cancelled)
	1	2.	(Cancelled)
·	1	3.	(Cancelled)
	1	4.	(Cancelled)
5	wb el	<b>&gt;</b> 5.	(Currently Amended) A computer-implemented system for protecting a
	2/	network, com	prising:
	3	a.	vulnerability detection system (VDS) for gathering information about the
	4		network to determine vulnerabilities of a plurality of hosts on the
\			network; and
)'	5	_	n intrusion detection system (IDS), cooperative with the VDS, for examining
	6	aı	network traffic responsive to the vulnerabilities of a host from the
	7		network trarile responsive to the value and the detect traffic indicative
	8		plurality of hosts as determined by the VDS to detect traffic indicative
	9		of malicious activity.
	-	1.	'
	1	2 E.	(Previously Presented) The system of claim \$, wherein the VDS is
	2	adanted to p	ather information about the network by sending data to the plurality of hosts
		and reneittin	ng responsive data from the plurality of hosts.
	3	and receiving	ig responsive dam seems !
	ı	3 7.	(Previously Presented) The system of claim 3, wherein the VDS is
	2	adapted to 9	gather information automatically provided by the plurality of hosts.
	4-		1
	1	¥ 8.	(Previously Presented) The system of claim 3, further comprising:
	_	χυ.	a vulnerabilities rules database, in communication with the VDS, for storing
	2	•	rules describing vulnerabilities of the plurality of hosts,
	3		Inter descripting Amingraphical and The Land

U.S. APPLICATION NO. 09/757,963

2 of 8

F&W CASE 6896 (AMD. D) 23327/06896/DOCS/1409368.1

	when	rein the VDS is adapted to analyze the gathered information with the rules				
4	to determine the vulnerabilities of the plurality of hosts.					
5		4				
4	5 9: (	(Previously Presented) The system of claim &, wherein the VDS is				
1	ا محر العدد معرف معرف	yze the gathered information with the rules to identify operating systems				
2	on the plurality of hosts and determine the vulnerabilities responsive to the respective					
3	on the plurality of hosts and documents and operating systems.					
4		. Ч				
1	6 <del>10</del> .	(Previously Presented) The system of claim 8, wherein the VDS is				
1	adapted to analyze the gathered information with the rules to identify open ports on the					
2	plurality of hosts and determine the vulnerabilities based on the open ports.					
3		4				
1	7 <del>11</del> .	(Previously Presented) The system of claim 8, wherein the VDS is				
2	adented to ana	lyze the gathered information with the rules to identify applications				
3	executing on the plurality of hosts and determine the vulnerabilities based on the					
4	applications.					
7	8	1				
1	عد -	(Original) The system of claim-5, further comprising:				
2	an	intrusion rules database, in communication with the IDS, for storing rules				
3		describing malicious activity,				
4	w!	beggin the IDS is adapted to analyze the network traffic with the rules to				
5		detect network traffic indicative of exploitations of the determined				
6		vulnerabilities.				
	9					
1	<del>13.</del>	(Original) The system of claim 5, wherein the IDS is adapted to detect				
2	traffic indica	tive of exploitations of only the determined vulnerabilities.				
	<b>—</b>					
1	14.	(Cancelled)				
	ιo	/ Single residence AVDS is adapted to undate				
1	15.	(Original) The system of claim 5; wherein the VDS is adapted to update				
2						
3	of malicious activity in response to the update.					

U.S. APPLICATION NO. 09/757,963

3 of 8

PAGE 8/13 \* RCVD AT 4/2/2004 3:30:31 PM [Eastern Standard Time] \* SVR:USPTO-EFXRF-1/1 \* DNIS:8729306 \* CSID:6509385200 \* DURATION (mm-ss):04-46

F&W CASE 6896 (AMD. D) 23327/06896/DOCS/1409368.1

10 11 (Original) The system of claim 15, wherein the VDS is adapted to update 16. the determined vulnerabilities in response to a change in the network.

17. network, comprising: 3 4 5

1

2

6

7

1

2

3

1

2

3

1

2

3

4

1

2

3

(Currently Amended) A computer-implemented method for protecting a

gathering information about the network to determine vulnerabilities of a plurality of hosts on the network; and cooperative with the step of gathering information, examining network traffic responsive to the determined vulnerabilities of a host from the plurality of hosts to detect network traffic indicative of malicious activity.

13

(Previously Presented) The method of claim 17, wherein gathering VS. information comprises sending data to plurality of hosts on the network and receiving responsive data from the plurality of hosts.

12

14 (Previously Presented) The method of claim 1/2, wherein gathering 19. information comprises receiving data automatically provided by the plurality of hosts on the network.

ک (Previously Presented) The method of claim 17, further comprising: 20: storing rules to describe vulnerabilities of the plurality of hosts, wherein determining vulnerabilities includes analyzing the gathered information with the rules.

ıŚ 16

(Previously Presented) The method of claim 20, wherein determining 21. vulnerabilities comprises analyzing the gathered information with the rules to identify operating systems on the plurality of hosts.

15 17 (Previously Presented) The method of claim 20, wherein determining 22. 1 vulnerabilities comprises analyzing the gathered information with the rules to identify 2 open ports on the plurality of hosts. 3

PAGE 9/13 \* RCVD AT 4/2/2004 3:30:31 PM [Eastern Standard Time] \* SVR:USPTO-EFXRF-1/1 \* DNIS:8729306 \* CSID:6509385200 \* DURATION (mm-ss):04-46

U.S. APPLICATION NO. 09/757,963

4 of 8

F&W CASE 6896 (AMD. D) 23327/06896/DOCS/1409368.1

15

(Previously Presented) The method of claim 20, wherein determining 1 vulnerabilities comprises comparing the gathered information against the rules to identify 2 applications on the plurality of hosts. 3 12 19 (Original) The method of claim 11, further comprising: 24. 1 storing rules describing malicious activity, 2 wherein detecting network traffic indicative of malicious activity comprises 3 analyzing the network traffic with the rules to detect traffic indicative 4 of exploitations of the determined vulnerabilities. 5 20 (Original) The method of claim 11, wherein examining network traffic 25. 1 consists of detecting traffic indicative of exploitations of only the determined 2 vulnerabilities. 3 (Cancelled) 26. 1 U (Previously Presented) The method of claim XI, further comprising: 27. 1 updating the determined vulnerabilities and detecting traffic indicative of 2 malicious activity in response to the update. 3 22 (Original) The method of claim 21, wherein the updating is responsive to a 28. 1 change in the network. 2 (Currently Amended) A computer program product, comprising: 29. a computer-readable medium having computer program logic embodied therein for protecting a network, the computer program logic: 3 gathering information about the network to determine vulnerabilities of a

U.S. APPLICATION NO. 09/757,963

5

6

7

8

5 of 8

F&W CASE 6896 (AMD. D) 23327/06896/DOCS/1409368.1

plurality of hosts on the network; and

cooperative with the step of gathering information, examining network traffic

of hosts to detect network traffic indicative of malicious activity.

responsive to the determined vulnerabilities of a host from the plurality

23

·	24	1 F ala: - 26			
1	<b>2</b> 6	(Previously Presented) The computer program product of claim 29,			
2	wherein gathering information comprises sending data to plurality of hosts on the				
3	receiving responsive data from the plurality of hosts.				
5		27			
	25 24.	(Previously Presented) The computer program product of claim 29,			
1	مار <i>م</i> مارست مارست	ring information comprises receiving data automatically provided by the			
2					
3	plurality of hosts on the network.				
1	26 32:	(Previously Presented) The computer program product of claim 29,			
2	further comprising:				
3	storing rules to describe vulnerabilities of the plurality of hosts,				
4	wherein determining vulnerabilities includes analyzing the gathered				
5		information with the rules.			
,	29	26			
1	ميود	(Previously Presented) The computer program product of claim 32,			
2	wherein determining vulnerabilities comprises analyzing the gathered information with				
3	the rules to identify operating systems on the plurality of hosts.				
,	_	24			
1	28 <del>34.</del>	(Previously Presented) The computer program product of claim 32,			
	wherein determining vulnerabilities comprises analyzing the gathered information with				
2	the rules to identify open ports on the plurality of hosts.				
3		genuity open posts on and programme 26			
	29 35	(Previously Presented) The computer program product of claim 32,			
1	35.	ermining vulnerabilities comprises comparing the gathered information			
2	wherein determining vulnerabilities comprises companies are garage and garage against the rules to identify applications on the plurality of hosts.				
3	against the	rules to identify applications of the planting of fine			
	zo	(Original) The computer program product of claim 25, further comprising:			
1	<del>36</del> .	(Original) The computer program product of same			

U.S. APPLICATION NO. 09/757,963

2

3

4

5

6 OF 8

of exploitations of the determined vulnerabilities.

F&W CASE 6896 (AMD. D) 23327/06896/DOCS/1409368.1

storing rules describing malicious activity,

wherein detecting network traffic indicative of malicious activity comprises

analyzing the network traffic with the rules to detect traffic indicative

2

31 (Original) The computer program product of claim 29, wherein examining 31. 1 network traffic consists of detecting traffic indicative of exploitations of only the verified 2 vulnerabilities. 3 (Cancelled) 1 23 (Previously Presented) The computer program product of claim 29, further 39%. 1 comprising: 2 updating the determined vulnerabilities; and 3 detecting traffic indicative of malicious activity in response to the update. 4 32 33 (Previously Presented) The computer program product of claim 39, 40. 1

wherein the updating is responsive to a change in the network.

U.S. APPLICATION NO. 09/757,963

7 of 8

F&W CASE 6896 (AMD. D) 23327/06896/DOCS/1409368.1